REMARKS

Applicant requests reconsideration of the subject application in view of the preceding amendments and the following remarks.

Claims 1-20 are pending in the application, with claims 1, 15, and 18 being the independent claims.

By this amendment, claims 1-15 and 18 have been amended to improve their form and to clarify features of the invention. Support for the amendments may be found in the application, as originally filed. No new matter has been added.

Art-Based Rejections

Claim 1 stands rejected under 35 U.S.C. § 103 as unpatentable over the article "IBM Cryptolopes, Super Distribution and Digital Rights Management" (Kaplan) in view of U.S. Patent No. 6,021,491 (Renaud). Claims 2-17 stand rejected under 35 U.S.C. § 103 as unpatentable over Kaplan in view of Renaud and further in view of U.S. Patent No. 5,894,320 (Vancelette). Claims 18-20 stand rejected under 35 U.S.C. § 103 as unpatentable over Kaplan in view of Renaud and further in view of the book "Applied Cryptography" (Schneier). Applicant traverses these rejections.

Independent Claim 1

In independent claim 1, the claimed invention recites a method for managing access to a scrambled event of a service provider featuring, *inter alia*, receiving in a device, in response to user selection of an event from a list of events, a digital signature and an encrypted message associated with the selected event. The digital signature is encrypted with a first key and the encrypted message is encrypted with a second key different from the first key. The encrypted message includes a descrambling key and event information. The method of claim 1 also includes authenticating in the device a

source of the digital signature and the encrypted message associated with the selected event by decrypting the digital signature in response to receiving the digital signature and the encrypted message. Upon authenticating the source, the encrypted message is decrypted in the device to obtain the descrambling key. The method also includes receiving in the device the selected event from the service provider, the selected event being scrambled using the descrambling key for preventing unauthorized access to the selected event, and descrambling in the device the selected event using the descrambling key.

Many of these features are not taught or suggested by Kaplan and Renaud, whether those documents are taken alone or in proper combination.

Kaplan teaches a cryptographic envelope used to disseminate for-sale information. As discussed beginning on page 3 of that document, the cryptographic envelope is a digital package including an abstract, encrypted parts, key records corresponding to the encrypted parts, encrypted fingerprinting and watermarking instructions, terms and conditions, and authenticity with digital signatures.

Renaud relates to digital signatures for data streams and data archives, and teaches a signature file that includes identifiers for one or more data files, provided with a digital signature created with a signature algorithm. The data files and signature file are then transferred or otherwise provided to a user, and the user verifies the digital signature in the signature file using a signature verifying algorithm. Once verified, the signature file can be used to verify each of the data files. From column 1, line 51 to column 2, line 6, Renaud discusses digital signatures generally and indicates that "digital signatures are basically mechanisms through which users may authenticate the source of a received data file," and "[i]n principle, such a verification process may provide a relatively high level of confidence in the authenticity of the source of the received data."

However, nowhere do Kaplan and Renaud teach or suggest at least receiving in a device an electronic list of events available from one or more sources, each event having a digital signature and an encrypted message associated therewith; receiving in the device, in response to user selection of one of the events, the digital signature and the encrypted message associated with the selected event, the digital signature being encrypted with a first key, the encrypted message being encrypted with a second key different from the first key, and the encrypted message comprising a descrambling key; and authenticating in the device a source of the digital signature and the encrypted message associated with the selected event by decrypting the digital signature in response to receiving the digital signature and the encrypted message, as now recited in independent claim 1.

Accordingly, Applicant submits that claim 1 recites features that patentably define Applicant's invention over the cited documents. Favorable reconsideration and withdrawal of the rejection of claim 1 are requested.

Independent Claim 15

Independent claim 15 recites a method for managing access between a device having a smart card coupled thereto and a service provider. The device receives an electronic program guide from a guide provider, the guide having a message and a digital signature associated with each event in the guide, the message being encrypted using a public key of the smart card and the digital signature being created using a private key of the guide provider. The method also includes selecting an event from the guide; receiving the encrypted message and the digital signature corresponding to the selected event; authenticating the guide provider by decrypting the digital signature using a public key of the guide provider, the guide provider public key being stored in the device; and passing the message to the smart card. In the smart card, the message is decrypted using a private key of the smart card to obtain event information and a symmetric key, the smart

card private key being stored within the smart card. The method also includes storing the event information in the smart card and updating account information based on the event information, receiving from the service provider the selected event, the selected event being scrambled using the symmetric key; and descrambling, in the smart card, the selected event using the symmetric key to generate a descrambled event.

Many of these features are not taught or suggested by Kaplan, Renaud and Vancelette, whether taken alone or in proper combination. Specifically, none of these documents is understood to teach or suggest passing a message to a smart card, decrypting the message in the smart card using a private key of the smart card to obtain event information and a symmetric key, the smart card private key being stored within the smart card; storing the event information in the smart card and updating account information based on the event information; or descrambling, in the smart card, the selected event using the symmetric key to generate a descrambled event.

The Office Action admits that these features are not taught or suggested by Kaplan or Renaud, and relies on Vancelette for their teaching.

Vancelette relates to a multi-channel television system with viewer-selectable video and audio in which a viewer can select among a choice of available camera angles and audio feeds when viewing a sporting event. At column 6, lines 57-65, Vancelette teaches preventing unauthorized viewers from accessing programming by encrypting the programming using one or more specified cryptographic programs. "Such encryption techniques are well known in the art." Column 6, lines 59-60. As understood, the encrypted packetized data stream is transmitted to set-top box, or the like, where it is demodulated and provided "to a demultiplexer/decryptor 530, where the encrypted data packets are decrypted and separated into two data paths. In a first path, control data packets such as packets 470 [] are provided to a microprocessor controller 540.... In the

other path, video and audio packets are provided to a processing and decompression function 555." Column 8, line 59 - column 9, line 10. The control data packets include code download packets, and object code from the code download packets is executed by the microprocessor 540. Column 9, lines 11-16. At column 9, lines 26-33, Vancelette contemplates that this code may also not be downloaded from the packetized data stream, but may be installed at the terminal via an access port and a smart card.

Vancelette is thus understood only to describe downloading code via insertion of a smart card into a set top box when the code is not provided in a packetized data stream. Nowhere does Vancelette teach or suggest passing a message encrypted using a public key of a smart card to a smart card, decrypting the message in a smart card, storing event information in the smart card, or descrambling an event in as smart card. Moreover, the Office Action makes no indication as to why these features would have been obvious from a combination of Kaplan, Renaud, and Vancelette.

Accordingly, Applicant submits that claim 15 patentably defines Applicant's invention over the cited documents, whether those documents are taken alone or in proper combination. Favorable reconsideration and withdrawal of the rejection of claim 15 respectfully are requested.

Independent Claim 18

Independent claim 18 recites a method for managing access between a device having a smart card coupled thereto and a service provider. Among other steps, the method includes passing a message to a smart card; decrypting, in the smart card, the message using a private key of the smart cart to obtain event information and a symmetric key, the smart card private key being stored within the smart card; storing the event information in the smart card and updating account information based on the event

information; and descrambling in the smart card the selected event using the symmetric key to generate a descrambled event.

The Office Action fails to consider these features, and none of the documents cited in the rejection of claim 18 even mentions a smart card. Accordingly, favorable reconsideration and withdrawal of the rejection of claim 18 respectfully are requested.

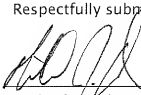
For the foregoing reasons, Applicant submits that independent claims 1, 15, and 18 are allowable over the cited patent documents. Favorable reconsideration and withdrawal of the rejections of these claims are requested.

The remaining claims depend from the independent claims. These claims are believed to be allowable by virtue of this dependency, and for reciting other patentable features of Applicant's invention. Favorable and independent consideration of the dependent claims respectfully are requested.

Applicant submits that this application is in condition for allowance. Favorable consideration and an early Notice of Allowance are requested.

Applicant's below-signed representative may be reached by telephone at (585) 232-6500 with any questions regarding this application. All written correspondence should continue to be forwarded to the address of record for this application.

Respectfully submitted,



Michael J. Didas, Registration No. 55,112
Customer Number 23387
HARTER SECREST & EMERY LLP
1600 Bausch & Lomb Place
Rochester, New York 14604
Telephone: 585-232-6500
Fax: 585-232-2152